

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平11-355558

(43)公開日 平成11年(1999)12月24日

(51)Int.Cl.<sup>8</sup>

H 0 4 N 1/387

5/92

識別記号

F I

H 0 4 N 1/387

5/92

審査請求 未請求 請求項の数 1 O L (全 16 頁)

(21)出願番号 特願平11-122464

(22)出願日 平成11年(1999)4月28日

(31)優先権主張番号 09/070-470

(32)優先日 1998年4月30日

(33)優先権主張国 米国 (US)

特許法第64条第2項ただし書の規定により図面第8図、  
第11図は不掲載とした。

(71)出願人 398038580

ヒューレット・パカード・カンパニー  
HEWLETT-PACKARD COM  
PANY

アメリカ合衆国カリフォルニア州パロアル  
ト ハノーバー・ストリート 3000

(72)発明者 ビング・ワー・ウォング

アメリカ合衆国 カリフォルニア, サニー  
ヴェイル, ノウルトン・ドライブ 1443

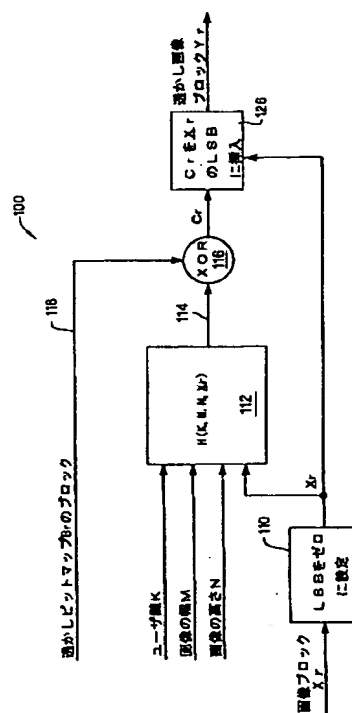
(74)代理人 弁理士 萩野 平 (外4名)

(54)【発明の名称】 透かし挿入装置

(57)【要約】

【課題】 ピクセル値のみならず画像サイズの変更も検  
出可能な、公開鍵あるいは秘密鍵透かし処理に使用でき  
るデジタル画像の透かし挿入装置を提供すること。

【解決手段】 画像ブロック  $X_r$  の少なくとも一つの所  
定ビットを修正して、修正済み画像ブロック  $X_z$  を生成  
する修正手段 110 と、暗号ハッシュ関数により値の摘  
要を計算しハッシュ出力 114 を出力する計算手段 11  
2 と、ハッシュ出力 114 を透かし 118 と組み合わ  
せ、合成画像ブロック  $C_r$  を生成する組み合わせ手段 1  
16 と、修正済み画像ブロック  $X_z$  の中に合成画像ブロ  
ック  $C_r$  を挿入し、透かし処理済み画像ブロック  $Y_r$  を出  
力する挿入手段 126 とから構成される。



## 【特許請求の範囲】

【請求項 1】 デジタル画像中に透かしを挿入する透かし挿入装置において、

画像ブロック  $X_r$  中の少なくとも 1 つの所定ビットを所定値に修正する手段であって、修正済み画像ブロックが  $X_r$  である修正手段と、

暗号ハッシュ関数を使用して値の摘要を計算する手段であって、該手段の出力がハッシュ出力であり、前記修正手段に電氣的に結合された計算手段と、

前記ハッシュ出力を透かしと組み合わせる手段であって、該手段の出力が合成画像ブロックであり、前記計算手段に電氣的に結合された組み合わせ手段と、

前記修正済み画像ブロック  $X_r$  に第 1 画像ブロックを挿入する手段であって、前記修正手段に電氣的に結合された挿入手段と、を備えたことを特徴とする透かし挿入装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、所有権の検証および／または認証の目的で画像中に透かしであるデジタル識別子を挿入し、また、受け取った画像中のデジタル識別子を抽出する技術に関する。

## 【0002】

【従来の技術】 デジタル透かしは、所有権の検証および／または認証の目的でデジタル識別子を抽出することができるように、画像中にデジタル識別子を挿入する技術である。所有権の検証とは、所有者に関連していると識別することができる透かし処理された画像から、デジタル識別子を抽出することができることを意味する。認証とは、透かし処理された画像に対するどのような変更も検出することができることを指す。デジタル透かしは、ワールドワイドウェブ (WWW) および電子商取引でのデジタル画像の使用の普及のため、ますます重要になっている。

【0003】 画像を見る者の視点から、透かしは 2 つの範疇、すなわち可視および不可視に分類することができる。可視透かし処理は、可視スタンプ、例えば会社ロゴが画像中に挿入される透かし処理手順のクラスをいう。このスタンプは、現在の米国ドル紙幣の透かしと同様に可視である。Braudaway 氏他の「Color Correct Digital Watermarking of Images」という名称の米国特許第 5,530,759 号公報に、元のデジタル画像中に可視の透かしを挿入する方法の記載がある。Braudaway 氏他は、透かしの位置に基づいて元画像の明るさ、または暗さを修正することを教示している。該公報に記載されている透かし挿入方法および透かし抽出方法にはランダムノイズ成分が含まれるため、許可されたユーザを除いては、元画像から透かしを除去する困難さが増す。

【0004】 不可視の透かしは、その結果生じる画像が元の透かし処理をしていない画像と視覚的に区別できな

いように、デジタル画像に加えられるデジタル識別子である。不可視の署名を、デジタル画像上の一連の画像処理操作により抽出または検出することができる。I. J. Cox 氏、J. Kilian 氏、T. Leighton 氏および T. Shamoon 氏の論文「Secure Spread Spectrum Watermarking for Multimedia」(Tech. Rep. 95-10, NEC Research Institute, 1995 年) は、デジタル画像中に不可視の透かしを挿入する方法を開示している。該論文は、画像の周波数領域表現への元画像の変換について記述している。該論文に記述された方法は、画像の周波数変換した表現から、視覚的に重要である  $N$  個の画像の周波数成分を選び、この元画像の周波数成分に透かし処理信号を透かしとして挿入する。

【0005】 所有権の検証を実施する一方法は、透かし処理された画像から適切なユーザ鍵によってのみ所望の透かしを抽出できるように、ユーザ鍵を透かしと関連付けることである。2 つの従来の透かし処理方法には、

(1) 所有者および受信者の両者が同じ秘密鍵を所有する必要がある秘密鍵透かし処理、および (2) 2 つの異なる鍵、すなわち、個人鍵およびそれに対応する公開鍵 (共通鍵) を使用する必要がある公開鍵透かし処理が含まれる。個人鍵は所有者だけが知っている。公開鍵は秘密である必要はなく、透かしを検出するために画像の受信者によって使用される。秘密鍵の透かしについての問題は、実際の伝送の前に、通常は、よりコストのかかる秘密の代替パスを介して鍵の交換を行わなければならないこと、または送信者と受信者とが近接しているときに取り決めなければならないことである。

【0006】 M. M. Yeung 氏および F. Mintzer 氏の論文「An invisible watermarking technique for image verification」(Proceedings of ICIP (米国、カリフォルニア州、サンタバーバラ) 1997 年 10 月) は、秘密鍵システムに関する認証透かし処理方法を開示している。該論文が教示する方法では、秘密鍵が乱数発生器と共に使用され、ルックアップテーブルを生成する。ルックアップテーブルは透かし抽出手順を規定し、同様に、いくつかの調整を経た元画像への透かし挿入ステップを提案する。透かし抽出ステップにおいて、抽出した透かしは、元画像が修正されたかどうか判定するために既知の透かしと比較される。該論文による技術は、透かし処理された画像のピクセル値に対する変更を検出できるが、クロッピング (cropping) アルゴリズムまたはある種のスケーリングアルゴリズムから生じる画像サイズの変更は検出しない。

## 【0007】

【発明が解決しようとする課題】 所有権の検証と認証との両方の目的に使用することができ、ピクセル値のみならず画像サイズの変更も検出でき、公開鍵あるいは秘密鍵透かし処理システムに使用される不可視の透かし処理技術が求められている。

## 3

【0008】本発明は、上記事情に鑑みてなされたもので、ピクセル値のみならず画像サイズの変更も検出でき、公開鍵あるいは秘密鍵透かし処理システムに使用でき、検証と認証との両方の目的に使用可能なデジタル画像中へ透かしを挿入する透かし挿入装置を提供することを目的とする。

## 【0009】

【課題を解決する手段】本発明は、所有権の検証と認証との両方の目的に使用でき、ピクセル値のみならず画像サイズの変更も検出でき、公開鍵あるいは秘密鍵透かし処理システムに使用される不可視のデジタル透かし処理技術を提供する。本発明は、画像所有者が使用する透かし挿入手順およびこれに対応する画像の受信者が使用する抽出手順を含む。透かし挿入手順は、修正済み画像ブロック、鍵および種々の画像パラメータのハッシュ関数を計算し、次いでハッシュ出力を1ブロックの透かしビットマップと組合せ、合成画像ブロックを生成する。好ましい実施形態では、修正済み画像ブロックは、そのLSBをゼロに設定した元の画像ブロックである。透かし処理された画像ブロックを生成する最後のステップとして、合成画像ブロックが修正済み画像のLSB中に挿入される。

【0010】透かし抽出手順では、透かし処理された画像ブロックを用いて、2つの異なる画像ブロック、すなわち透かし処理された画像ブロックのLSBをゼロに設定した第1画像ブロックと、透かし処理された画像ブロックのLSBを抽出した第2画像ブロックとを生成する。第1画像ブロック、鍵および種々の画像パラメータは、ハッシュ関数の入力として使用される。透かし抽出工程のためのハッシュ関数への入力は、透かし挿入工程のためのハッシュ関数への入力とは異なっているが、透かし挿入と抽出との両方に使用される暗号ハッシュ関数は同一でなければならない。ハッシュ関数が異なる場合、この透かしを適切に抽出することができず、抽出した透かし画像がノイズとして現れる。

【0011】透かし抽出手順は、ハッシュ関数を使用して値の摘要を計算し、ハッシュ出力を生じる。ハッシュ出力は、好ましくは排他的論理和を使用して、第2画像ブロックと組み合わせられる。第2画像ブロックを有する組み合わせられたハッシュ出力の結果は、抽出された透かしの1ブロックである。

【0012】上述の挿入および抽出方法は、同じ秘密鍵が透かし挿入と抽出との両方に使用される秘密鍵暗号化のために使用される。代替の実施形態では、前記方法が、画像の完全性および所有権を公開鍵を使用して検証することができるように修正される。この代替の実施形態において、透かし挿入手順では、公開鍵暗号化ステップが、ハッシュした関数を透かしビットマップと組み合わせるステップの後に入れられる。さらに、透かし抽出手順では、可逆排他的論理和論理関数を使用して、公開

## 4

鍵解読ステップが透かしを抽出する前に入れられる。このようなシステムでは、画像の所有者は個人鍵 $K'$ を用いて透かしを挿入する。透かし抽出手順では、いずれの個人も、バイナリ(binary)透かしを抽出するために、(個人鍵 $K'$ に対応する)公開鍵 $K$ を使用することができ、これによって透かし処理された画像に対して行われたあらゆる変更が示される。

【0013】本発明は、秘密鍵と公開鍵との両方の透かし処理システムで透かし処理された画像に対するあらゆる変更を検出する認証技術を提供する。変更の検出は、例えば、画像が法律上の証拠として使用される場合、および画像の電子商取引において、この画像が売り手から買い手に配送される場合に、画像に対する変更がないことを画像の買い手に保証することができる。この画像のいずれかの部分が変更された場合、本発明による透かし抽出手順は変更された画像の特定の部分を示す出力を返す。透かし処理された画像が切り取られた場合、この抽出手順はランダムノイズに似た出力を返し、切り取られた画像が有効でないことを表す。

【0014】本発明の性質および利点は、本明細書の以後の発明の実施の形態および図面を参照すればさらに理解できよう。

## 【0015】

【発明の実施の形態】本発明は、 $M \times N$ ピクセルの画像 $X_{m,n}$ の中にデジタル識別子を埋め込み、抽出して、同じサイズの透かし処理された画像 $Y_{m,n}$ を形成する技術を提供する。図1および図2に、本発明の第1の実施形態に基づく透かし挿入装置および透かし挿入方法を示す。図4および図5に、本発明の第1の実施形態に基づく透かし抽出装置および透かし抽出方法を示す。図4および図5に示す透かし抽出装置および透かし抽出方法は、図1および図2に示した透かし挿入装置および透かし挿入方法と一緒に使用すべきである。

【0016】図1のブロック図を参照すると、透かし挿入装置を実施するためのブロック図が示される。図2には、図1に示す透かし挿入装置に対応する方法のステップを示すフローチャートが示されている。図1を参照すると、本発明に基づいて、元の入力デジタル画像中への透かし挿入を実施するための透かし挿入装置100は、画像ブロック $X_I$ 中の少なくとも1つの所定ビットを修正して、修正済み画像ブロック $X_F$ を生成する修正手段100と、修正手段110が電氣的に結合され、暗号ハッシュ関数を使用して値の摘要(digest)を計算し、ハッシュ出力114を出力する計算手段112と、計算手段112に電氣的に結合され、ハッシュ出力114を透かし118と組み合わせ、該組み合わせによる出力が合成画像ブロックである組み合わせ手段116と、修正手段110に電氣的に結合された、修正済み画像ブロック $X_F$ の中に合成画像ブロック( $C_F$ )を挿入する挿入手段126とを含む。

【0017】図2のフローチャートを参照すると、好ましい実施形態では、元の入力デジタル画像の中に透かしを挿入するための方法は、少なくとも1つの $I \times J$ のブロック中に画像ブロック $X_r$ を区分するステップ(150)と、各 $I \times J$ ブロックごとに、該ブロックの少なくとも1つの所定ビットを所定値に修正するステップであって、前記修正済み画像ブロックが $X_r$ であるステップ(152)と、暗号ハッシュ関数を使用して値の摘要を計算するステップ(154)と、前のステップで計算したハッシュ出力を透かしビットマップ $B_r$ と組み合わせるステップであって、その場合、ハッシュ出力を透かし $B_r$ と組み合わせるステップの出力は、合成画像ブロック $C_r$ であるステップ(156)と、修正済み画像 $X_r$ 中に値 $C_r$ を挿入するステップ(158)とを含む。

【0018】図2に示すステップは、図1に示す実施ブロック図に対応する。例えば、値の摘要を計算するステップ(ステップ154)は、図1の実施ブロック112に対応する。言い換えると、値の摘要を計算するステップは、ブロック112によって実行される。同様に、ステップ152はブロック110に対応し、ステップ156はブロック116に対応し、ステップ158はブロック126に対応する。図2に、図1のステップのフローチャートを示すが、図1に示すブロック図は、各ステップおよび一連のステップから生じる入力および出力を明示する。

【0019】所定ビットを所定値に設定する手段への入力は、1ブロックの元の入力画像 $X_{m,n}$ である。好ましい実施形態では、元の入力画像 $X_{m,n}$ はサイズ $M \times N$ のグレースケール画像である。代替の実施形態では、元の入力画像はカラー画像である。カラー画像の場合、図1、図2、図3、図4、図5、図12、図13、図14および図15に示す同じ技術を、RGBカラー空間または、例えばYUV等の他の任意のカラー空間のどちらかにある画像のカラー平面に独立して適用することができる。

【0020】好ましい実施形態では、画像 $X_{m,n}$ は、 $I \times J$ のピクセルのブロック中に区分される。一実施形態では、他のブロックサイズも可能であるが、本願記載の区分されたブロックは、 $8 \times 8$ である。さらに、元の画像を $I \times J$ のピクセルブロックに区分するステップが必要になる(これは、画像を1つのブロック中に区分することに等しく、画像ブロックは $I = M$ および $J = N$ のブロックサイズを有する)。しかし、全体の画像に対してブロックを1つとするのは好ましくない。元の入力画像の区分は、画像を認証する時にローカライゼーション

(localization)を維持する助けとなる。さらに、区分は、この画像を見る者が、画像の変更が生じた位置をより明確に見る助けになる。

【0021】 $X_{m,n}$ 中に埋め込むべき透かしを表す2レベル画像を $a_{m,n}$ とする。 $a_{m,n}$ は、 $X_{m,n}$ と同じサイズ

である必要はないことに留意されたい。 $a_{m,n}$ から、

( $X_{m,n}$ と同じサイズの)サイズ $M \times N$ の別の2レベル画像 $b_{m,n}$ を形成することができる。画像 $a_{m,n}$ を、 $X_{m,n}$ と同じサイズの画像に変換する多くの方法がある。例えば、 $b_{m,n}$ は、 $a_{m,n}$ をタイル化(tiling)すること、すなわち定期的に $a_{m,n}$ を所望のサイズに置き換えることによって形成されてもよい。別の可能性は、所望のサイズの $b_{m,n}$ が得られるように、 $a_{m,n}$ の境界に全てゼロ(または、全て1)を添付することである。

10 【0022】 $I \times J$ のピクセルブロックの中に区分された元の入力画像 $X_{m,n}$ について、

$$X_r = x_{iI+kJ+j+1} \quad (\text{但し、} 0 \leq k \leq I-1, 0 \leq l \leq J-1)$$

を画像 $X_{m,n}$ から得られる1ブロックのサイズ $I \times J$ であるとする。話を簡単にするために、単一インデックス $r$ を使用して、この画像中の $r$ 番目のブロックを示している。透かしビットマップ118に対するバイナリ画像 $b_{m,n}$ 内の対応するブロックが、下式で表される。

$$B_r = b_{iI+kJ+j+1} \quad (\text{但し、} 0 \leq k \leq I-1, 0 \leq l \leq J-1)$$

$I$ および $J$ は、 $I, J \leq p$ を満足するならば、任意の数にすることができることに留意されたい。但し、 $p$ はハッシュ関数112のサイズである。

【0023】画像ブロックの少なくとも1つの所定ビットを所定値に修正する修正手段110への入力が、画像 $X_{m,n}$ の $r$ 番目のブロックである。好ましい実施形態では、設定中のビットは、そのブロックのLSBである。このブロックのLSBを修正すると、最小の可視画像ゆがみが生じるが、これは不可視の透かしのための重要な要因である。図1に示す実施形態が好ましいが、画像ブロック $X_r$ を修正するための代替の方法を使用することもできる。しかし、代替の方法を実施する場合でさえ、透かし挿入工程中の画像ブロック $X_r$ を修正する(手段110、ステップ152a)ものと同じ方法を、図4および図5に示す透かし抽出工程の透かし処理された画像ブロック $Y_r$ を修正する(手段210、ステップ252a)ものにも使用しなければならないことは重要である。

【0024】図1に示す実施形態では、画像ブロック $X_r$ は、画像ブロックのLSBをゼロに設定することによって修正される。ステップ152で実施された実施形態の代替の実施形態では、LSB以外のビット(あるいは、1群のビット)は、所定値に設定される。図1に示す実施形態では、システム設計者によって決定された値を変更することができるが、この所定値はゼロである。前述のように、所定値および所定ビットの位置が、システム設計者によって変更できるが、図1で規定された透かし挿入手順に使用されたものと同じ所定ビットおよび所定値を、図4および図5で規定された透かし抽出手順にも使用しなければならないことは重要である。言い換

えれば、元の入力画像のブロックの所定ビットを所定値に設定する修正手段110が、所定ビットとしてその画像のLSBを、かつその所定値として値ゼロを使用する場合、図4の所定ビットを設定する手段210は、所定ビットとしてその画像のLSBを、またその所定値として値ゼロを使用しなければならない。

【0025】図3に、画像ブロック $X_r$ を修正するための様々な代替形態を示す。(図1に示す)第1の実施形態では、各ブロックごとに、画像ブロック $X_r$ の所定ビットが所定値に設定される。しかし、代替の実施形態では、各ブロックごとに所定ビットが放棄される(ステップ152b)。所定ビットが放棄される場合、合成画像ブロック $C_r$ が、好適にはこの所定ビットに挿入される。第3の代替の実施形態では、画像ブロックは1パターンのビットに基づいて修正することができる(ステップ152c)。所定のブロックがあるパターンに基づいて修正される場合、合成画像ブロック $C_r$ が、好適にはこのパターンのビットに挿入される(ステップ158)。図3には、画像ブロック $X_r$ を修正するための3つだけの可能な代替形態を示す。画像ブロック $X_r$ を修正するために、他の代替形態も可能である。重要なことは、画像ブロック $X_r$ が修正されることである。合成画像の少なくとも一部が、修正済み画像ブロック $X_r$ の修正されたビットに挿入されることが好ましい。

【0026】画像ブロックのブロックの所定ビットを修正する手段の出力は $X_r$ である。 $X_r$ は、暗号ハッシュ関数を使用して、値 $K, M, N, X_r$ の摘要を計算する手段と、 $C_r$ を $X_r$ の所定ビットに挿入する手段との両方に入力される。図1および図2を参照すると、暗号ハッシュ関数を使用して、値の摘要を計算する手段への入力、 $K$ (ユーザ鍵)、 $X_r$ (修正済み画像ブロック)、 $M$ (元の入力の幅)および $N$ (元の入力ブロックの高さ)である。

【0027】図1および図2を参照すると、暗号ハッシュ関数を使用して、値 $K, M, N, X_r$ の摘要を計算するステップが示されている。暗号ハッシュ関数は、様々なハッシュ関数から選択される。好ましい実施形態では、周知のMD5関数またはその変形が使用される。MD5関数は、例えば、R.L.Rivest氏の論文「The MD5 Message Digest Algorithm」(Internet RFC 1321, 1992年4月)に記述されている。本開示の残りの部分では、MD5をハッシュ関数として使用するが、他の代替実施形態では他の暗号関数も使用できる。

【0028】本発明に記載する実施形態では、 $K$ は秘密暗号化鍵であり、 $X_r$ は修正した元の入力画像ブロックであり、 $M$ は元の入力画像の幅であり、 $N$ は元の入力画像の高さである。暗号ハッシュ関数 $H(S) = (d_1, d_2, \dots, d_p)$ を考えてみる。該式で、 $S$ は任意の長さのデータ列を表し、 $d_i$ はハッシュ関数のバイナリ出力ビットであり、 $p$ はこの出力ビット列のサイズである。

入力ビット列 $S$ およびそれに対応する出力 $(d_1, \dots, d_p)$ が与えられたものとして、同じ出力 $(d_1, \dots, d_p)$ にハッシュされる任意の長さの別の入力ビット列を見つけることは、計算上実行不可能である。このMD5ハッシュアルゴリズムを使用して、任意のデータ列が、長さ128、すなわち $p=128$ のビットアレイ中にハッシュされる。別の暗号関数が使用される場合、長さ $p$ は異なることがある。好ましい実施形態では、不等式 $p \geq IJ$ が満たされる。

10 【0029】 $K$ をビット列からなるユーザ鍵とする。好ましい実施形態では、各ブロックのデータ $X_r$ について、それに対応するブロック $X_r$ を形成する。但し、 $X_r$ 中の各要素は、最下位ビットがゼロに設定されることを除いて、 $X_r$ 中の対応する要素に等しい。各ブロックごとに、ハッシュ $H(K, M, N, X_r) = (d_1, d_2, \dots, d_p)$ を計算する。

【0030】次いで、ハッシュ出力中の最初の $IJ$ ビットを選択し、サイズ $I \times J$ の長方形アレイ $d_{m,n}$ を形成する。

20 【0031】ハッシュ出力 $d(d_1, d_2, \dots, d_p)$ および透かし処理されたビットマップ $B_r$ のブロックが、ハッシュ出力を透かしと組み合わせる手段に入力される。透かしの抽出と挿入との両方の工程は、このハッシュ出力を透かし $B_r$ と組み合わせるステップを含む。このハッシュ出力114を透かし118と組み合わせるステップは、ビットごとの論理演算を使用して実行される。これによって、透かし挿入と抽出との両方の工程のための容易な処理が可能になる。好ましい実施形態では、図1および図2に示すように、ビットごとの論理演算は排他的論理和関数である。

30 【0032】図1を参照すると、ハッシュ出力アレイが $B_r$ と組み合わせられ、ピクセル排他的論理和演算による1ピクセルを使用して、新しいバイナリブロック $C_r$ が形成される。すなわち、 $c_{m,n} = b_{m,n} \text{ XOR } d_i$ を形成する。該式において、XORは排他的論理和演算を示す、 $c_{m,n}$ は $C_r$ 中の要素であり、 $b_{m,n}$ は $B_r$ 中の要素であり、 $d_i$ はハッシュ出力 $d$ の要素である。

40 【0033】好ましい実施形態では、透かし処理された画像生成前の最後のステップは、修正済み画像 $X_r$ の中に値 $C_r$ を挿入することである。修正済み画像ブロック $X_r$ では、この画像ブロックの少なくとも1ビットが所定値に設定される。通常、 $C_r$ は修正されたビットのみに挿入される。修正された各ビットが挿入ビット $C_r$ に対応することが好ましいが、代替の実施形態では、ビット $C_r$ はこの画像ブロックの各修正されたビットに対応せず、したがって、 $C_r$ の値はどの修正されたビットの中にも挿入されない。この好ましい実施形態では、この画像ブロックのLSBはゼロに設定されるように修正され、 $C_r$ は $X_r$ のLSBの中に挿入され、ある値の $C_r$ が各修正されたビットの中に挿入される。

【0034】好ましい実施形態では、 $c_{m,n}$ をブロック $X_r$ の最下位ビットに置いて、出力ブロック $Y_r$ を形成する。この手順は、各ブロックのデータに対して繰り返され、全ての出力ブロック $Y_r$ は、透かし処理された画像 $Y_{m,n}$ を形成するように一緒にアセンブルされる。組み合わせた出力ブロック $C_r$ および修正済み画像 $X_r$ は、 $C_r$ を $X_r$ の所定ビットに挿入する手段への入力である。 $C_r$ を $X_r$ の所定ビットに挿入する手段の出力は、出力画像ブロック $Y_r$ である。出力画像ブロック $Y_r$ は、透かし処理された画像ブロックである。

【0035】図4を参照すると、図1および図2に示す透かし挿入装置および透かし挿入方法とあいまって使用される、透かし抽出装置200のブロック図が示されている。透かし抽出工程は、画像ブロック $Y_r$ から透かし $B_r$ を抽出して、この透かしを引き出す。図4を参照すると、透かし抽出装置200は、少なくとも1つの所定ビットを所定値に修正する修正手段210と、透かし処理された画像ブロック $Y_r$ から少なくとも1つの所定ビットを抽出する抽出手段218と、修正手段210に電氣的に結合された、暗号ハッシュ関数を使用して値の摘要を計算する計算手段212と、抽出手段218に電氣的に結合された、ハッシュ出力値214を抽出された画像ブロック $E_r$ と組み合わせる組み合わせ手段216とを含む。

【0036】図4および図5に示すフローチャートを参照すると、デジタル画像 $Y_r$ から透かしを抽出する方法が示されていて、各 $I \times J$ のブロックのために、透かし処理された画像 $Y_r$ の少なくとも1つの所定ビットを所定値に修正するステップであって、修正した透かし処理された画像 $Y_r$ が $Y_r$ であるステップ(252)と、透かし処理された画像から少なくとも1つの所定ビットを抽出するステップ(254)と、暗号ハッシュ関数を使用して値の摘要を計算するステップ(256)と、このハッシュ出力を画像ブロック $E_r$ と組み合わせるステップ(258)とを含む。

【0037】図4を参照すると、暗号ハッシュ関数を使用して値 $K$ 、 $M$ 、 $N$ 、 $Y_r$ の摘要を計算するためのブロックへの入力は、 $K$ (ユーザ鍵)、 $M$ (元の画像の画像幅)、 $N$ (元の画像の画像高さ)および $Y_r$ (画像ブロックの1つの所定ビットを所定値に設定するように修正した透かし処理済み画像ブロック)である。したがって、透かし処理された画像ブロックの1つの所定ビットを所定値に修正するステップ(ステップ252)が、暗号ハッシュ関数を使用して、値 $K$ 、 $M$ 、 $N$ 、 $Y_r$ の摘要を計算するステップ(ステップ256)の前に実行されなければならない。

【0038】抽出した透かしを得た後、この抽出した透かしは、(コンピュータ画像比較プログラム等を使用して、視覚的に)適当な透かしと比較することができる。例えば、この適当な透かしは、透かしを比較するため

に、より早い時期に受信者に送信された画像であってもよい。2つの透かし間に偏差がある場合、偏差の位置が透かし処理された画像内の変更された領域を示す。

【0039】図6～図11に、図1、図2、図4および図5に基づく透かし挿入装置および透かし挿入方法と透かし抽出装置および透かし抽出方法を使用して、生成した画像によって現された特性をより明確に示す。例えば、図6および図7によれば、本発明が記載する透かし方法が、不可視の透かし処理を実施することを明瞭にしている。図6を参照すると、透かし挿入前の元の画像を示す。図7に、図1および図2に記述した透かし挿入装置および透かし挿入方法を使用して透かし処理された透かし処理済み画像を示す。図6と図7を比較すると、この2つの画像間に視覚的に観測可能な差がないので、生成した透かしは不可視の透かしである。

【0040】図8および図9によって明確に示される別の特性は、正しいユーザ鍵が適切な透かしの抽出のために必要なことである。正しいユーザ鍵 $K$ を使用し、透かし抽出手順を図7に適用する場合、適切な透かしの存在を示す出力画像図8が得られる。これと対照的に、例えば、画像がマークされないか、不正な鍵が使用されるか、元の画像が切り取られる場合に生じる可能性があるランダムノイズに似た出力画像を図9に示す。画像がマークされない場合、すなわち、画像が透かしを含まない場合、透かし抽出手順は、図9に示すようにランダムノイズに似た出力を返す。同様に、不正な鍵を適用する場合(例えば、鍵を知らない場合)、透かし抽出手順はランダムノイズに似た出力を返す。別の例として、透かし処理された画像が切り取られて、この切り取られた画像上に透かし抽出手順を適用する場合、その出力はランダム雑音に似るはずである。

【0041】図10に、ガラスを含むことによって修正された図7の透かし処理された画像を示す。透かし処理された画像に修正(ガラスの添加)を加えた特定の領域を示す、図10から抽出された透かしを図11に示す。透かし処理された画像の中のあるピクセルを変更すると、この変更の特定の位置が透かし抽出手順の出力に反映される。図10に、ガラスが図7上に貼られた画像を示す。また、図11に、変更が加えられた特定の領域を示す図10から抽出された透かしを示す。

【0042】生じる疑問は、透かしがこの画像の最下位ビットに置かれる場合、この透かしは安全であるかということである。この透かしは、認証目的のため、すなわち、この画像に対するどんな変更も検出するように設計されていることを想起されたい。誰かが、この画像のいくつかのビット平面を変更することによって透かしを除去しようとする場合、透かし抽出手順がこの変更を検出することになる。

【0043】非常に重要な問題は、誰かがこの方式の中に透かしを偽造することが可能であるかどうかということ

とである。画像ブロック $B_r$ を考えてみる。誰かが、画像ブロックが $B_r$ になるように、この画像ブロック中のピクセルのいくつかまたは全てを変更したいと仮定する。2つの画像ブロック中のピクセル値が、 $H(K, M, N, B_r) = H(K, M, N, \underline{B}_r)$ を満たす必要がある。

【0044】すなわち、両方の画像ブロックから生成された摘要は同一でなければならない。これは、MD5アルゴリズム等の暗号ハッシュ関数の特性のために、計算的に実行不可能であると見なされる。

【0045】図1、図2、図3、図4および図5に示した第1の実施形態では、透かし挿入および透かし抽出を秘密鍵システムに関して説明した。図12、図13、図14および図15に示した第2の実施形態は、透かし挿入および透かし抽出を公開鍵システムに対して提供する。

【0046】図12に、公開鍵システムに関する、元の入力デジタル画像への透かし挿入を実施するための透かし挿入装置のブロック図を示す。図12に示すブロック図は、図1に示すシステムの修正版であり、公開鍵暗号化を含むように修正が加えられている。同様に、図14に示すブロック図は、図14に示す抽出装置が公開鍵解読を含むように修正されていることを除いて、図4に示すシステムを修正したものである。

【0047】公開鍵暗号化を含むために加えられた修正を除いて（例えば、ハッシュ関数および電気接続への入力が修正された）、一般に図1、図2および図3に対して行われた説明を、図12および図13に対しても行うことができる。同様に、図4および図5に対して行われた説明を、図14および図15に対して適用する。例えば、画像ブロック $X_r$ が図3に示す代替に基づいて修正される可能性があるという、図1に対して行われた説明は、図12に対しても当てはまる（実施ブロック910は、図1に示す代替に基づいて修正される）。

【0048】図12に、公開鍵システムを実施する第2の実施形態に基づく透かし挿入装置のブロック図を示す。また、図13に、図12に示す透かし挿入装置に対応するステップのフローチャートを示す。第1の実施形態に規定された画像と同様に、公開鍵システムに関して、 $M \times N$ ピクセルのサイズを有するグレースケール画像 $x_{m,n}$ を想定する。透かし処理された画像 $y_{m,n}$ を得るために $x_{m,n}$ にバイナリの不可視の透かし画像 $b_{m,n}$ を挿入したい。第1の実施形態と同様に、透かし挿入および透かし抽出は、いくつかのブロックの画像データ上に実行される。便宜上、画像ブロックのサイズを、 $8 \times 8$ と選択する。

【0049】図12を参照すると、公開鍵システム用の透かし挿入装置900は、画像ブロック $X_r$ の少なくとも1つの所定ビットを修正する修正手段910と、修正手段910に電氣的に結合された、ハッシュ出力 $P_r$ を

出力し（914）、暗号ハッシュ関数を使用して値の摘要を計算する計算手段912と、計算手段912に電氣的に結合された、ハッシュ出力914を透かし918と組み合わせる組み合わせ手段916と、組み合わせ手段916に電氣的に結合された公開鍵暗号化手段922と、修正手段910に電氣的に結合された、画像 $\underline{X}_r$ のブロックの1つの所定ビットに暗号化した出力および透かし（ $W_r$ ）を挿入する挿入手段926とを含む。

【0050】図13に、図12に示す挿入装置に対応するステップのフローチャートを示す。図13のフローチャートを参照すると、公開鍵システムに関して、デジタルの元の入力画像に透かしを挿入する方法は、 $I \times J$ のブロックに元の画像 $X_r$ を区分するステップ（950）と、各 $I \times J$ ブロックについて、画像ブロックの少なくとも1つの所定ビットを修正するステップであって、修正済み画像が $\underline{X}_r$ であるステップ（952）と、暗号ハッシュ関数を使用して値の摘要を計算するステップ（954）と、前のステップで計算したハッシュ出力を透かし $B_r$ と組み合わせるステップの出力が合成画像 $C_r$ であるステップ（956）と、合成画像 $C_r$ を暗号化するステップであって、暗号化した画像が $W_r$ であるステップ（958）と、修正済み画像ブロック $\underline{X}_r$ に値 $W_r$ を組み入れるステップ（960）とを含む。

【0051】秘密鍵システム用の透かし挿入に関して記述した方法と同様に、 $X_r$ は画像 $x_{m,n}$ 内の $r$ 番目のデータブロックを示す。次に、1つの所定ビット（最下位ビット）が所定値ゼロに設定されることを除いて、 $\underline{X}_r$ の中の各要素が $\underline{X}_r$ の中の対応する要素と等しい、対応するブロック $X_r$ が形成される。 $H(\cdot)$ は、MD5アルゴリズム等の暗号ハッシュ関数であるとする。このハッシュ関数は、次のように計算される。 $H(M, N, \underline{X}_r) = (p^r_1, p^r_2, \dots, p^r_s)$

【0052】該式において、 $p^r_i$ はハッシュ関数からの出力ビットを示し、 $s$ は使用される特定のハッシュ関数に依存する出力ビットのサイズである。例えば、MD5に対して、 $s = 128$ である。

【0053】ビットストリーム $P_r$ から第1の $IJ$ ビットを表すと、下式となる。

【0054】

【数1】

$$P_r \triangleq (p^r_1, p^r_2, \dots, p^r_{IJ})$$

【0055】 $P_r$ は $b_{m,n}$ のビットごとの論理関数であり、通常は排他的論理和関数を使用して、 $b_{m,n}$ 中の対応するブロック $B_r$ と組み合わせられる。すなわち、 $C_r = P_r \text{ XOR } B_r$ を計算する。但し、XORは2つのブロック間の要素ごとの排他的論理和演算を示す。最後に、公開鍵暗号システムで $C_r$ を暗号化して、 $W_r = E_{K'}(C_r)$ を生じる。該式において、 $E(\cdot)$ はこの公開鍵システムの暗号化関数であり、 $K'$ は個人鍵であ



る。次いで、バイナリブロックのデータ $W_r$ は最下位ビットのデータブロック $X_r$ 中に埋め込まれ、透かし処理された画像の中にブロック $Y_r$ を形成する。

【0056】図14に、図12および図13に示す透かし挿入装置および透かし方法と共に使用される透かし抽出装置のブロック図を示す。図15に、図14に示す透かし検出装置に使用される、透かし抽出方法のフローチャートを示す。図14に示す透かし検出装置1000は、透かし処理された画像 $Z_r$ のブロックの少なくとも1つの所定ビットを所定値に修正して、修正済み画像ブロック $Z_r$ を生成する修正手段1010と、画像 $Z_r$ から1つの所定ビットを抽出する抽出手段1018と、修正手段1010が電氣的に結合された、暗号ハッシュ関数を使用して値の摘要を計算する計算手段1012と、抽出手段1018に電氣的に結合され、出力が解読された画像ブロック $U_r$ である公開鍵解読手段1020と、ハッシュ出力値を解読された画像ブロック $U_r$ と組み合わせる手段であって、ハッシュ出力を修正した画像ブロック $Z_r$ と組み合わせる該手段が、公開鍵解読手段1020と計算手段1012とに電氣的に結合されている組み合わせ手段1016とを含む。

【0057】抽出手順では、画像ブロック $Z_r$ が、2つの異なる画像を生成するために使用される。好ましい実施形態では、最下位ビットがゼロアウト(zero out)されたことを除いて、第1画像 $G_r$ が最下位ビットを含み、他の画像 $Z_r$ がピクセル値を含む。次いで、 $M$ 、 $N$ および $Z_r$ のハッシュを計算し、出力の最初の $I$   $J$ ビットを $Q_r$ で示す。公開鍵解読アルゴリズムを使用して、透かし挿入手順に使用した個人鍵 $K'$ に対応する公開鍵 $K$ で $G_r$ を解読する。すなわち、 $U_r = D(G_r)$ を計算する。最後に、要素ごとの排他的論理和手順を使用して、出力ブロック $O_r = Q_r \text{ XOR } U_r$ を計算する。

【0058】公開鍵を用いた透かし挿入および透かし抽出の実施では、ハッシュ関数としてMD5を、暗号化および解読のためにRSA公開鍵暗号化アルゴリズムを使用した。透かし処理された画像ブロックと画像サイズとの両方が、透かしの挿入以後、変更されなかった場合、すなわち、 $Z_r = Y_r$ の場合、 $Z_r = X_r$ および $G_r = W_r$ である。これは、 $P_r = Q_r$ および $U_r = C_r$ であることを意味する。したがって、出力バイナリ画像 $O_r$ はブロック $B_r$ と同一である。そうでない場合は、これに該当せず、ハッシュ関数の性質のため、出力ブロック $O_r$ はランダムノイズとほとんど変わらないであろう。結果として、このアルゴリズムは、ピクセル値やブロックレベルに対してのあらゆる変更を検出することができる。

【0059】図14に、図12および図13に示す透かし挿入装置と透かし挿入方法と組み合わせられて使用される透かし抽出装置のブロック図を示す。図15を参照すると、公開鍵暗号化システムに関して、デジタル画像 $Y_r$ から透かしを抽出する方法は、各 $I \times J$ のブロックご

とに、透かし処理された画像 $Z_r$ の少なくとも1つの所定ビットを所定値に修正するステップであって、修正した透かし処理済み画像 $Z_r$ が $Z_r$ であるステップ(1050)と、透かし処理された画像 $Z_r$ から、少なくとも1つの所定ビットを抽出するステップであって、この抽出した画像ブロックが $G_r$ であるステップ(1054)と、暗号ハッシュ関数を使用して値の摘要を計算するステップ(1052)と、公開鍵解読関数 $D_k(\cdot)$ を使用して $G_r$ を解読するステップであって、この解読された画像ブロックが $U_r$ であるステップ(1056)と、ハッシュ出力をこの解読された画像ブロック $U_r$ と組み合わせるステップ(1058)とを含むことを示す。

【0060】図16に、図1および図2に示す秘密鍵検証方法の特性を要約した実験結果の要約を示す。同様に、図17に、図12および図13に示す公開鍵検証方法の特性を要約した実験結果の要約を示す。図16および図17を参照すると、所有権の検証を実施する一方式は、所望の透かしのみを適当なユーザ鍵で透かし処理された画像から抽出することができるよう、ユーザ鍵を透かしと関連付けることである。ユーザが不正な鍵を使用したか、または透かし処理されていない画像で透かし抽出手順を実行した場合、ユーザはランダムノイズに似た画像を得る。

【0061】図1、図2、図3、図4、図5、図12、図13、図14および図15に示すブロック図およびフローチャートは、ハードウェアまたはソフトウェアのいずれか、あるいは両方の組合せで実施される。例えば、図1のブロック図を参照すると、ハッシュ関数の計算(値の摘要の計算)はソフトウェアで実施することができるが、排他的論理和関数(116)および画像ブロックの所定ビットの修正は、ハードウェアで実行することができる。あるいは、別の実施形態では、図1に示すブロック図の実施は、全部ソフトウェアで実施することができるはずであり、ソフトウェアはコンピュータが読取り可能な媒体に記憶され、コンピュータシステム上で動作するように適合される。

【0062】図18に、本発明に基づく透かし方法のステップを実施するソフトウェアプログラムを実行するように適合されたコンピュータシステムの高レベルのブロック図を示す。中央演算処理装置(CPU)1311はバス1312に接続され、このバス1312はランダムアクセスメモリ(RAM)1313、読取り専用メモリ(ROM)1314、入出力(I/O)アダプタ1315、通信アダプタ1316、ユーザインターフェイスアダプタ1317およびディスプレイアダプタ1318に接続される。RAM1313とROM1314は、通常、ユーザおよびシステムのデータとプログラムを記憶する。通常は、本発明を実施するソフトウェアプログラムは記憶媒体上に常駐し、CPU上で実行される。

【0063】上記説明は例示的なものであり、制限する



ものではないことを理解されたい。例えば、本発明は、同じサイズの透かし処理された画像 $Y_{m,n}$ を形成するために、 $M \times N$ 個のピクセルの画像 $X_{m,n}$ 中にデジタル識別子を埋め込むための透かし処理技術を提供する。代替の実施形態では、透かし処理された画像は、画像 $X_{m,n}$ とは異なるサイズである。したがって、本発明の範囲は、添付の特許請求の範囲と前記特許請求の範囲が受ける権利のある全範囲の均等物と共に参照して決定されるべきである。

【0064】以下に本発明の実施の形態を要約する。

1. デジタル画像中に透かしを挿入する透かし挿入装置において、画像ブロック $X_r$ 中の少なくとも1つの所定ビットを所定値に修正して、修正済み画像ブロック $X_r$ を生成する第1の修正手段と、前記第1の修正手段に電氣的に結合され、暗号ハッシュ関数を使用して値の摘要を計算して、ハッシュ出力を出力する第1の計算手段と、前記第1の計算手段に電氣的に結合され、前記ハッシュ出力を透かしと組み合わせて、合成画像ブロックを出力する第1の組み合わせ手段と、前記第1の修正手段に電氣的に結合され、前記修正済み画像ブロック $X_r$ に第1画像ブロックを挿入する挿入手段と、を備えた透かし挿入装置。

【0065】2. 前記第1画像ブロックが前記合成画像ブロック $C_r$ である上記1記載の透かし挿入装置。

【0066】3. 前記第1画像ブロックが暗号化された画像ブロック $W_r$ である上記1記載の透かし挿入装置。

【0067】4. 前記第1の組み合わせ手段が前記挿入手段に電氣的に結合される上記2記載の透かし挿入装置。

【0068】5. 前記第1の修正手段が前記画像ブロック $X_r$ のLSBを修正する上記1記載の透かし挿入装置。

【0069】6. 前記第1の組み合わせ手段がXOR論理ブロックである上記1記載の透かし挿入装置。

【0070】7. 前記第1の修正手段が前記画像ブロックの各カラー平面ごとに独立して少なくとも1つの所定ビットを修正する上記1記載の透かし挿入装置。

【0071】8. 前記第1の組み合わせ手段と前記挿入手段との両方に電氣的に結合された暗号化手段をさらに備えた上記3記載の透かし挿入装置。

【0072】9. デジタル画像から透かしを抽出する透かし抽出装置において、透かし処理された画像の少なくとも1つの所定ビットを所定値に修正する第2の修正手段と、透かし処理された画像ブロックから少なくとも1つの所定ビットを抽出する抽出手段と、前記第2の修正手段に電氣的に結合され、暗号ハッシュ関数を使用して値の摘要を計算して、ハッシュ出力を出力する第2の計算手段と、前記第2の計算手段に電氣的に結合された第2の組み合わせ手段と、を備えた透かし抽出装置。

【0073】10. 前記第2の組み合わせ手段が前記抽

出手段に電氣的に結合される上記9記載の透かし抽出装置。

【0074】11. 前記抽出手段および前記第2の組み合わせ手段に電氣的に結合された解読手段をさらに備えた上記9記載の透かし抽出装置。

【0075】12. 前記修正手段が前記画像ブロックの最下位のビットを修正する上記9記載の透かし抽出装置。

【0076】13. デジタル画像中に透かしを挿入する透かし挿入方法において、少なくとも1つの $I \times J$ のブロック中に画像ブロック $X_r$ を区分けする区分けステップと、各 $I \times J$ ブロックごとに、各 $I \times J$ ブロックの少なくとも1つの所定ビットを所定値に修正して、修正済み画像ブロックが $X_r$ を生成する修正ステップと、暗号ハッシュ関数を使用して値の摘要を計算する計算ステップと、前のステップで計算したハッシュ出力を透かしビットマップ $B_r$ と組み合わせて、合成画像ブロック $C_r$ を出力する組み合わせステップと、前記修正済み画像ブロック $X_r$ に第1画像ブロックを挿入する挿入ステップと、有する透かし挿入方法。

【0077】14. 前記第1画像ブロックが前記合成画像ブロック $C_r$ である上記13記載の透かし挿入方法。

【0078】15. 前記第1画像ブロックが暗号化された画像ブロック $W_r$ である上記13記載の透かし挿入方法。

【0079】16. 暗号化した画像ブロック $W_r$ を生成する前記合成画像ブロックを暗号化する暗号化ステップをさらに有する上記13記載の透かし挿入方法。

【0080】17. 前記画像ブロック $X_r$ の少なくとも1つの所定ビットが前記所定ビットを放棄することによって修正される上記13記載の透かし挿入方法。

【0081】18. 前記画像ブロック $X_r$ の少なくとも1つの所定ビットを修正する前記修正ステップが、複数のビットが所定のパターンのビットを所定値に設定することによって修正する上記13記載の透かし挿入方法。

【0082】

【発明の効果】以上に詳述したように、本発明のデジタル画像中に透かしを挿入する透かし挿入装置は、画像ブロック $X_r$ 中の少なくとも1つの所定ビットを所定値に修正する手段であって、修正済み画像ブロックが $X_r$ である修正手段と、暗号ハッシュ関数を使用して値の摘要を計算する手段であって、該手段の出力がハッシュ出力であり、修正手段に電氣的に結合された計算手段と、ハッシュ出力を透かしと組み合わせる手段であって、該手段の出力が合成画像ブロックであり、計算手段に電氣的に結合された組み合わせ手段と、修正済み画像ブロック $X_r$ に第1画像ブロックを挿入する手段であって、修正手段に電氣的に結合された挿入手段とから構成されていることにより、透かしを抽出する透かし抽出装置を用いて透かしを抽出するとき、ピクセル値が変更された場合

のみならず画像サイズの変更の場合も検出でき、公開鍵あるいは秘密鍵透かし処理システムに使用できる。

【図面の簡単な説明】

【図 1】本発明の第 1 の実施形態に係る透かし挿入装置を示すブロック図である。

【図 2】図 1 に示す透かし挿入装置に対応する透かし挿入方法を示すフローチャートである。

【図 3】図 2 に示された画像ブロック  $X_r$  を修正するステップ 152 の代替を示す説明図である。

【図 4】図 1、図 2 および図 3 に示す透かし挿入装置および透かし挿入方法と共に使用される透かし抽出装置を示すブロック図である。

【図 5】図 1、図 2 および図 3 に示す透かし挿入方法と共に使用される透かし抽出方法を示すフローチャートである。

【図 6】透かし挿入前の元の画像を示す図である。

【図 7】透かし挿入装置および透かし挿入方法を使用して透かし処理を行った画像を示す図である。

【図 8】正しいユーザ鍵  $K$  が使用されたとき、透かし抽出手順の適用後の抽出した透かし出力画像を示す図である。

【図 9】画像がマークされていない、不正な鍵が適用されている、または元の画像が切り取られているなどの場合に生じることのある、ランダムノイズに似た抽出した透かし出力画像を示す図である。

【図 10】ガラスを付加することによって修正した図 7 の透かし処理を行った画像を示す図である。

【図 11】ガラスの付加によって透かし処理された画像に対する修正が行われた特定の領域を示す図 10 から抽出された透かしを示す図である。

【図 12】公開鍵システムを実施する本発明の第 2 の実施形態に係る透かし挿入装置を示すブロック図である。

【図 13】図 12 に示す透かし挿入装置に対応する透か

し挿入方法を示すフローチャートである。

【図 14】図 12 および図 13 に示す透かし挿入装置および透かし挿入方法と共に使用される透かし抽出装置を示すブロック図である。

【図 15】図 12 および図 13 に示す挿入装置および透かし挿入方法と共に使用される透かし抽出方法を示すフローチャートである。

【図 16】図 1 および図 2 に示す秘密鍵検証方法の特性を要約した実験結果の要約を示す図である。

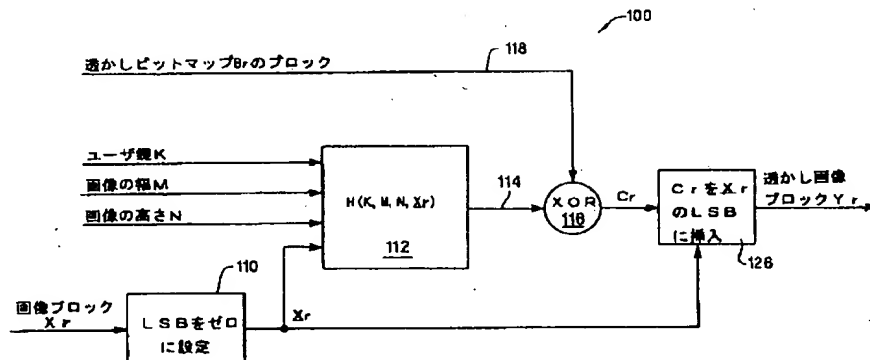
【図 17】図 12 および図 13 に示す公開鍵検証方法の特性を要約した実験結果の要約を示す図である。

【図 18】本発明の実施形態に係る透かし挿入方法のステップを実施するソフトウェアプログラムを実行するように適合されたコンピュータシステムを示す高レベルのブロック図である。

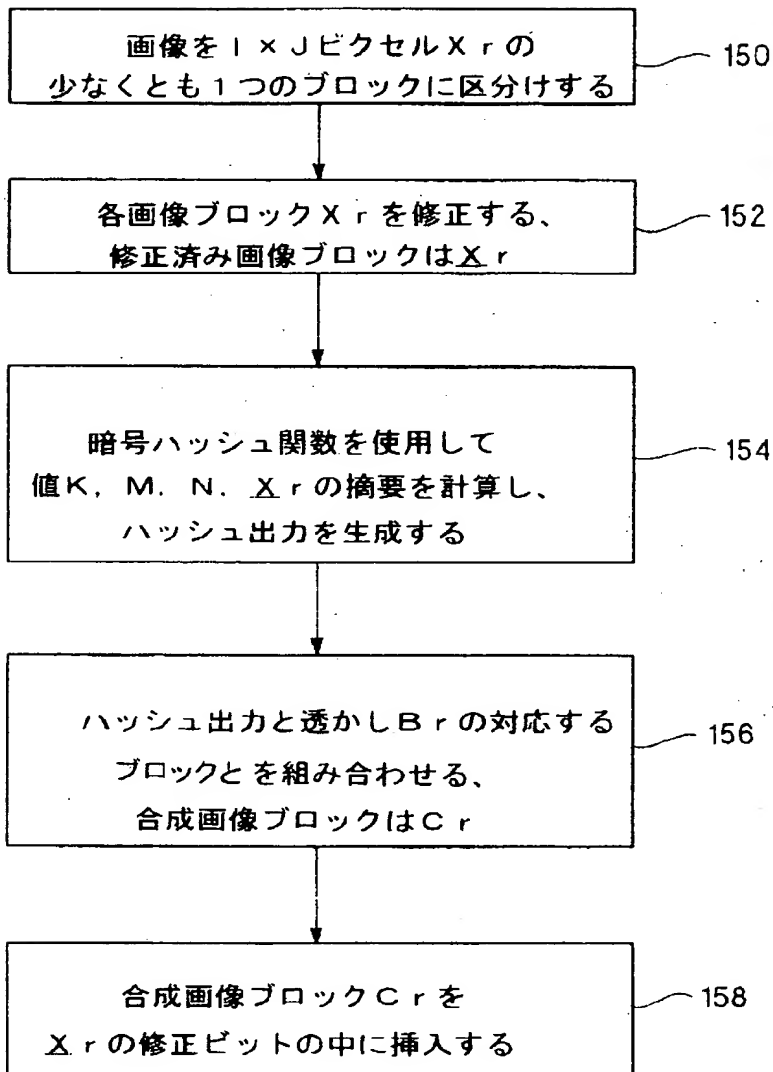
【符号の説明】

100, 900 透かし挿入装置  
110, 210, 910, 1010 修正手段  
112, 212, 912, 1012 計算手段  
116, 216, 916, 1016 組み合わせ手段  
126, 926 挿入手段  
218, 1018 抽出手段  
200, 1000 透かし抽出装置  
922 公開鍵暗号化手段  
1020 公開鍵解読手段  
1311 CPU  
1313 RAM  
1314 ROM  
1315 I/Oアダプタ  
1316 通信アダプタ  
1317 ユーザインターフェイスアダプタ  
1318 ディスプレイアダプタ

【図 1】



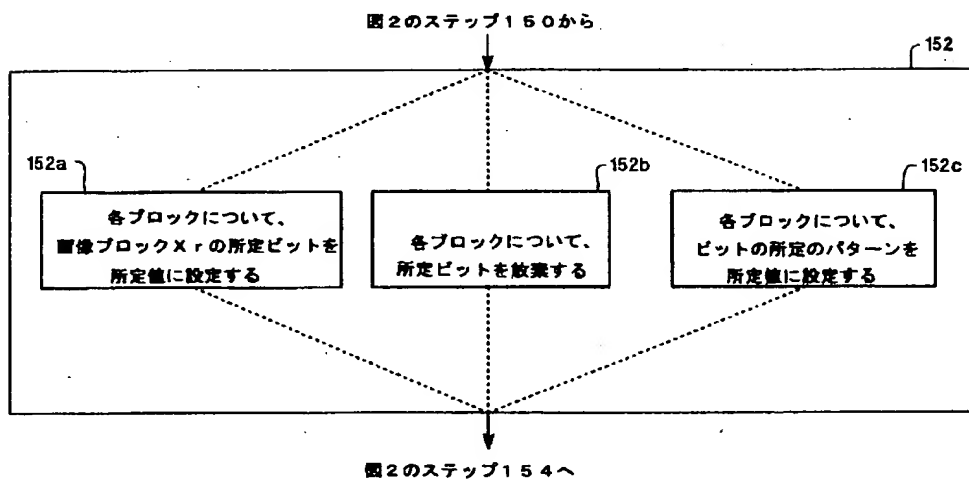
【図 2】



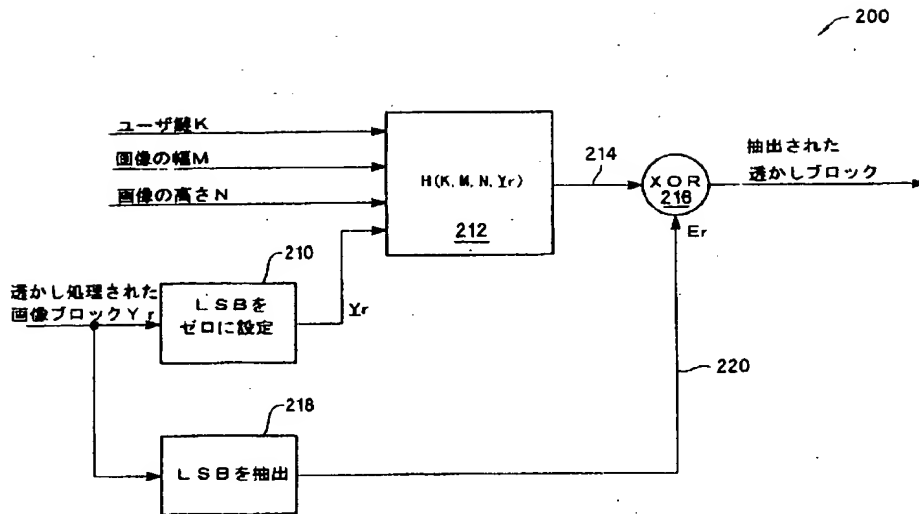
【図 6】



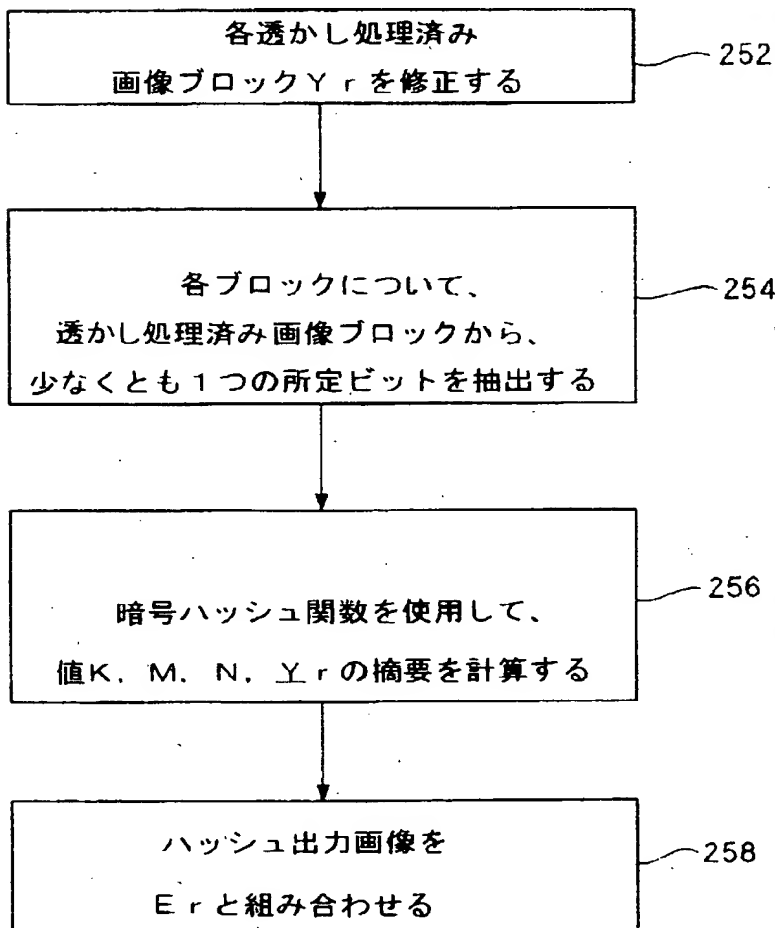
【図 3】



【図 4】



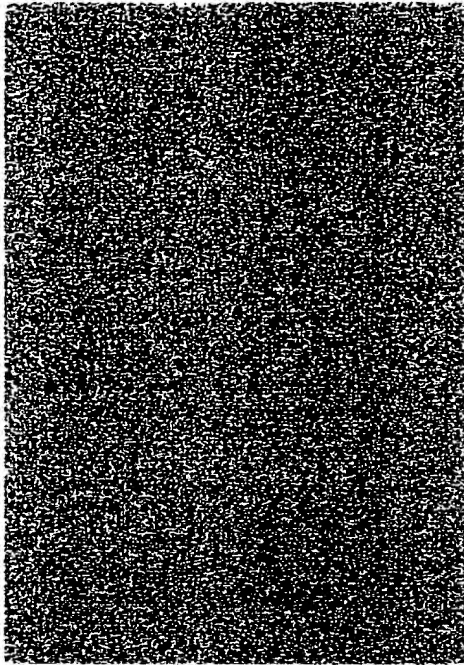
【図 5】



【図 7】



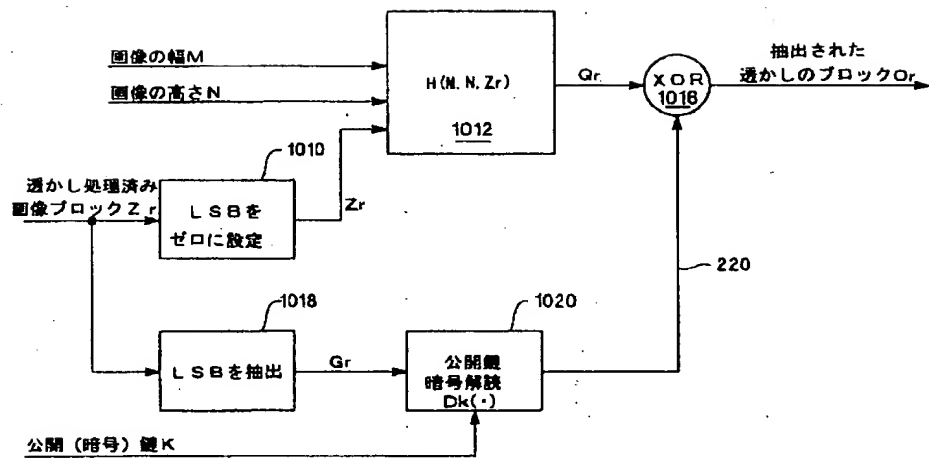
【図 9】



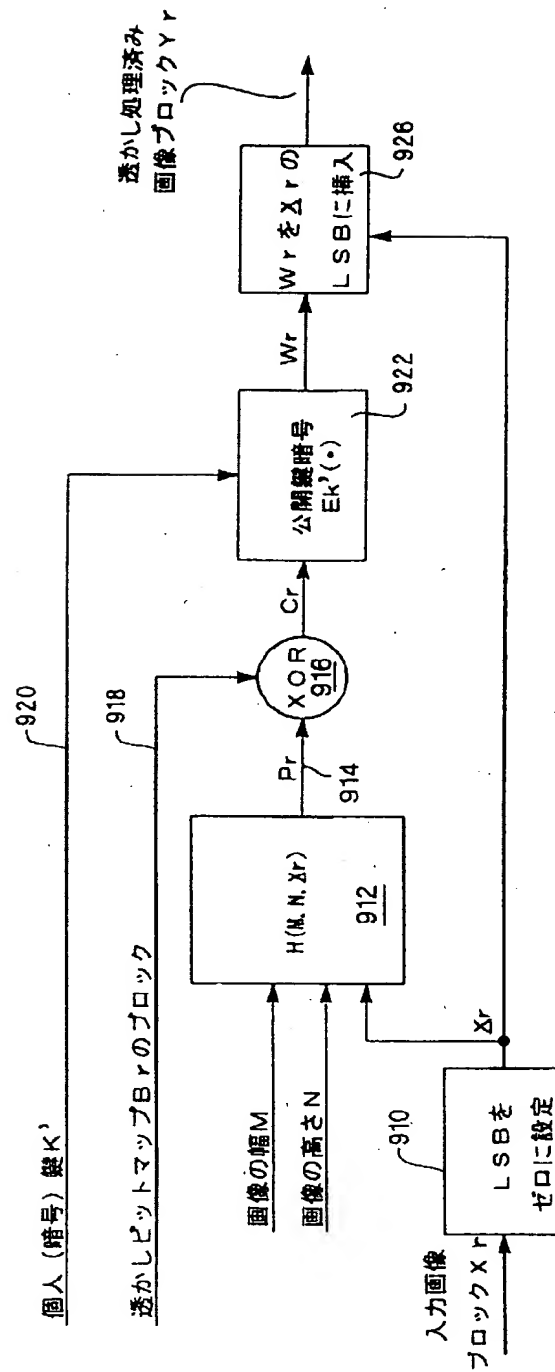
【図 10】



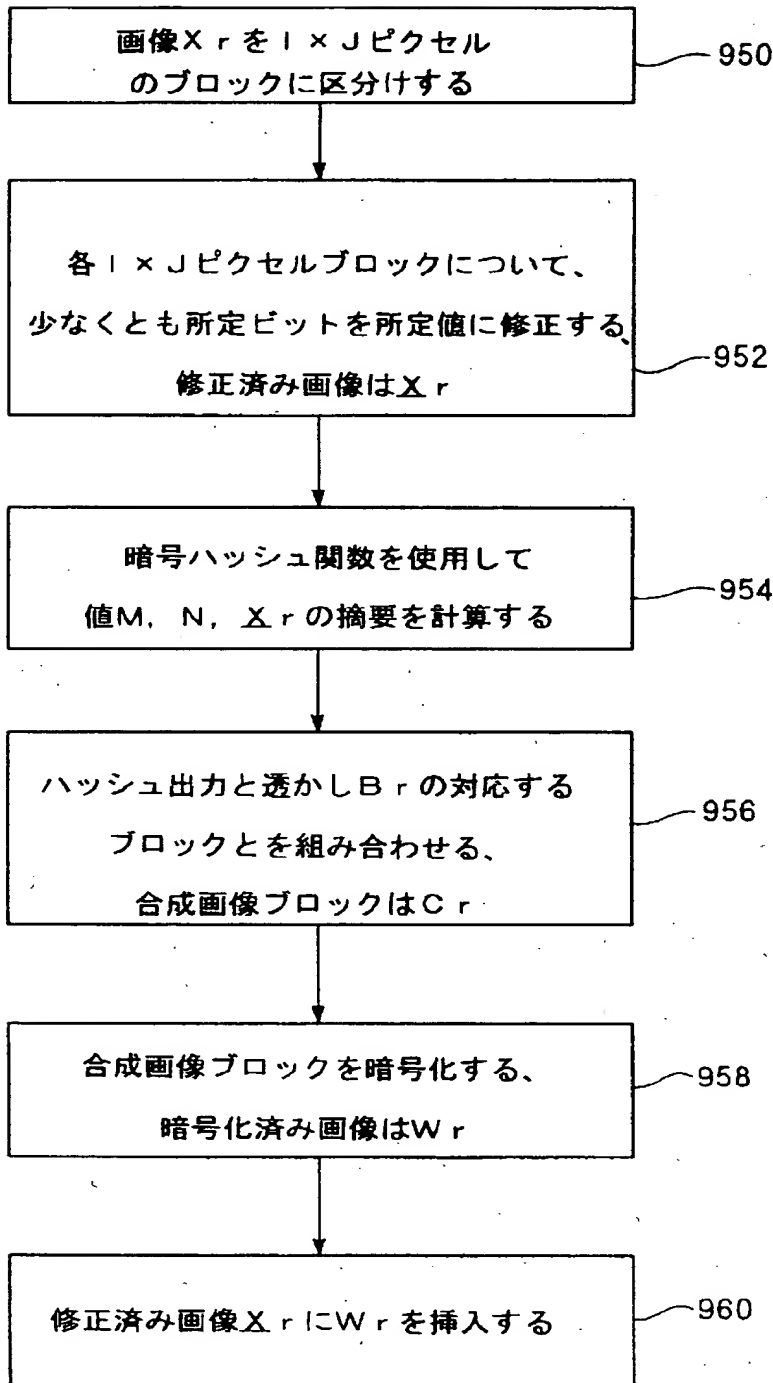
【図 14】



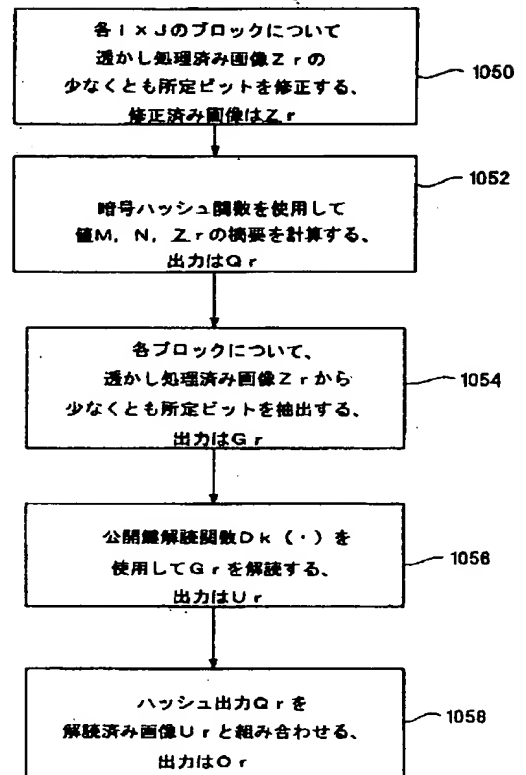
【図 1 2】



【図 13】

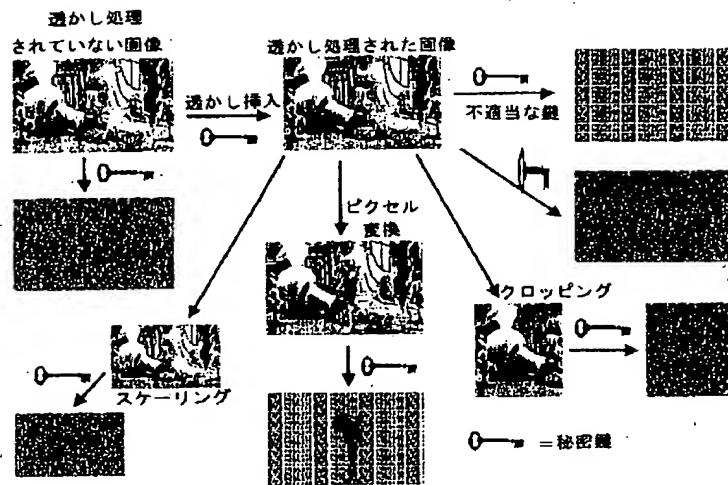


【図 15】

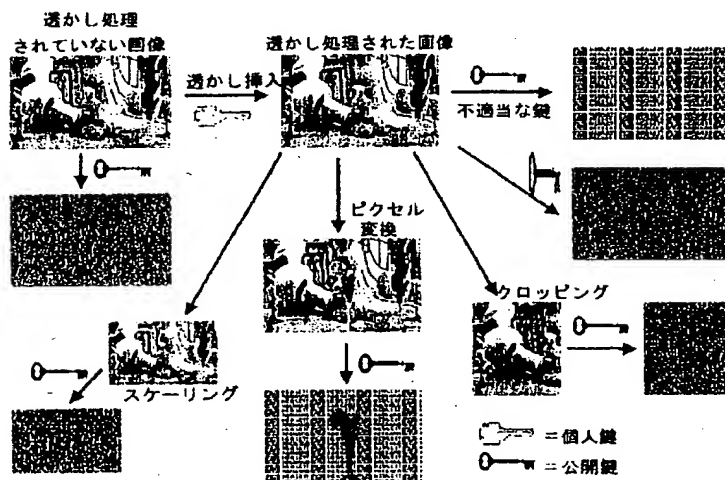




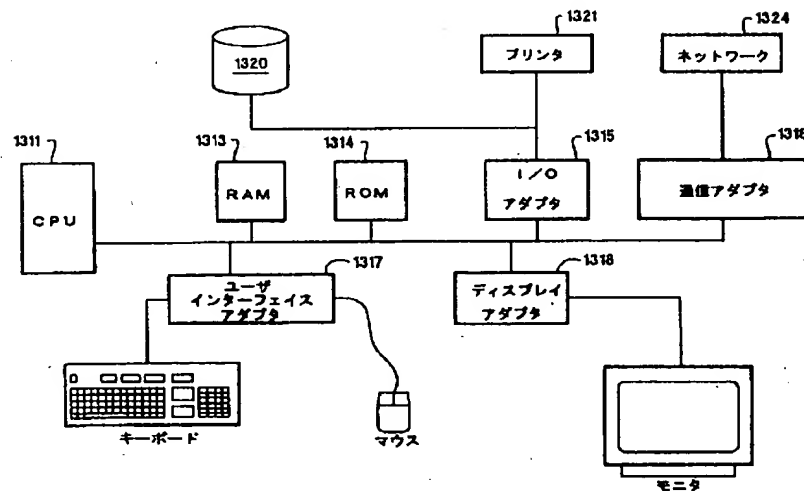
【図 16】



【図 17】



【図 18】



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☒ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**